GVNW CONSULTING, INC.

8050 SW WARM SPRINGS STREET
SUITE 200
P.O. BOX 2330
TUALATIN, OR 97062
TEL 503.612.4400
FAX 503.612.4401
www.gvnw.com

February 22, 2010

FILED ELECTRONICALLY

Ms. Marlene H. Dortch
Secretary
Federal Communications Commission
445 12th Street, SW
Washington, D.C. 20554

re: EB Docket No. 06-36

Dear Ms. Dortch:

On behalf of Triangle Telephone Cooperative Association, Inc., Form 499 Filer ID 801114 pursuant to §64.2009(e) of the Commission's rules, I am attaching the CPNI Compliance Certificate and the Accompanying Statement as required.

Please contact me with any questions at 503-612-4400.

Sincerely,

Carsten Koldsbaek

Carsten Koldsbaek
Consulting Manager

Enclosures

Copies to:
Federal Communications Commission
Enforcement Bureau
445 – 12th Street SW
Washington, DC 20554

Best Copy & Printing Inc.
445 – 12th Street, Suite CY-B402
Washington, DC 20554

Annual 47 C.F.R. § 64.2009 (e) CPNI Certification

EB Docket 06-36

Annual 64.2009(e) CPNI Certification for 2010 covering the prior calendar year 2009

1. Date filed : February 22, 2010

2. Name of company(s) covered by this certification: Triangle Telephone Cooperative Association, Inc.

3. Form 499 Filer ID: 801114

4. Name of signatory: Richard Stevens

5. Title of signatory : General Manager

6. Certification :

I, Richard Stevens, certify that I am an officer of the company named above, and acting as an agent of the company, that I have personal knowledge that the company has established operating procedures that are adequate to ensure compliance with the Commission's CPNI rules. *See* 47 C.F.R.§ 64.2001 *et seq.*

Attached to this certification is an accompanying statement explaining how the company's procedures ensure that the company is in compliance with the requirements (including those mandating the adoption of CPNI procedures, training, recordkeeping, and supervisory review) set forth in section 64.2001 *et seq.* of the Commission's rules.

The company has not taken actions (*i.e.*, proceedings instituted or petitions filed by a company at either state commissions, the court system, or at the Commission against data brokers) against data brokers in the past year.

The company has not received customer complaints in the past year concerning the unauthorized release of CPNI.

The company represents and warrants that the above certification is consistent with 47 C.F.R. § 1.17 which requires truthful and accurate statements to the Commission. The company also acknowledges that false statements and misrepresentations to the Commission are punishable under Title 18 of the U.S. Code and may subject it to enforcement action.

Signed 

Attachments: Accompanying Statement explaining CPNI procedures

CPNI Compliance Accompanying Statement:
Year: 2010 covering the prior calendar year 2009

Triangle Telephone Cooperative Association, Inc.

This accompanying statement explains how Triangle Telephone Cooperative Association, Inc.'s operating procedures ensure that the company is in compliance with the rules governing CPNI as found in Subpart U – Customer Proprietary Network Information – Part 64 of Title 47 of the Code of Federal Regulations.

Triangle Telephone Cooperative Association, Inc. adheres to all CPNI rules as stated in section 64.2001 – 64.2011 concerning the proper use of our customer's CPNI. Specifically, our notice for use of CPNI approval process meets all requirements as listed in Section 64.2008. To further protect our customer's privacy, we have implemented all safeguards required in Section 64.2009. This includes:

- The implementation of a system by which the status of a customer's CPNI approval can be clearly established prior to the use of CPNI;
- The training of appropriate personnel as to when they are, and are not, authorized to use CPNI and the documentation of this training;
- The implementation of an express disciplinary process for CPNI violations up to and including termination;
- The maintenance of a record, for at least one year, of our own, and our affiliates' sales and marketing campaigns ;
- The establishment of a supervisory review process regarding carrier compliance with the federal CPNI rules for outbound marketing situations; and
- The establishment of annual certification by a corporate officer with personal knowledge of Triangle Telephone Cooperative Association, Inc.'s policies and procedures to ensure compliance with the federal CPNI rules.
- The establishment of procedures for notification of the Commission of any instance where opt-out mechanisms, do not work properly, to such a degree that consumers' inability to opt-out is more than an anomaly.

Triangle Telephone Cooperative Association, Inc. has on file with the FCC its CPNI Manual, without the sample Forms, as further detailed explanation of how its procedures ensure that it is in compliance with the rules in Subpart U of Part 64, of Title 47 of the Code of Federal Regulations.

TRIANGLE TELEPHONE COOPERATIVE ASSOCIATION, INC.

CENTRAL MONTANA COMMUNICATIONS, INC.

TRIANGLE COMMUNICATION SYSTEM, INC.

CPNI

COMPLIANCE MANUAL AND

OPERATING PROCEDURES

Approved by:

Signed by Richard Stevens March 30, 2009
General Manager Date

Effective: March 30, 2009

TABLE OF CONTENTS

Definitions

Account information. Information that is specifically connected to the customer's service relationship with a telecommunications carrier, including such things as an account number or any component thereof, the telephone number associated with the account, or the bill amount.

Address of record. An address, whether postal or electronic, that a carrier has associated with the customer's account for at least 30 days.

Affiliate. A person that (directly or indirectly) owns or controls, is owned or controlled by, or is under common ownership or control with, another person to own an equity interest (or the equivalent thereof) of more than 10 percent.

Aggregate Customer Information. Collective data that relates to a group or category of services or customers from which individual customer identities and characteristics have been removed.

Breach. When a person, without authorization or exceeding authorization, has intentionally gained access to, used, or disclosed CPNI.

Call detail information. Any information that pertains to the transmission of specific telephone calls, including, for outbound calls, the number called, and the time, location, or duration of any call and, for inbound calls, the number from which the call was placed, and the time, location, or duration of any call.

Communications-related services. Telecommunication services, information services typically provided by telecommunications carriers, and services related to the provision or maintenance of customer premises equipment.

Customer. A person or entity to which a telecommunications carrier is currently providing service.

Customer premises equipment (CPE). Equipment employed on the premises of a person (other than a carrier) to originate, route, or terminate telecommunications.

Customer Proprietary Network Information. The term "customer proprietary network information" means –

(A) information that relates to the quantity, technical configuration, type, destination, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier and that is made available to the carrier solely by virtue of the carrier-customer relationship; and

(B) information contained in the bills pertaining to telephone exchange service or telephone toll service received by a customer of a carrier; except that such term does not include subscriber list information.

Data broker. A person or business that offers for sale CPNI obtained by pretexting.

Data bureau. A company that provides information technology services to telecommunications carriers, specifically billing services and customer record detail. Data bureaus typically have access to call detail CPNI (see Independent contractor).

FCC. Federal Communications Commission.

Independent contractor. Any person or business that may provide services to telecommunications carriers. This includes, but is not limited to; joint venture partners and independent contractors for the purposes of marketing communications-related services to a customer; billing services; customer record detail; central office equipment vendors; engineering; and construction. Independent contractors typically have access to call detail and/or non-call detail CPNI.

Information services typically provided by Telecommunications Carriers. Information services that telecommunications carriers typically provide such as Internet access or voice mail services. The term as used in this Manual shall not include retail consumer services provided using Internet website (such as travel reservation services or mortgage lending services), whether or not such services may other wise be considered to be information services.

Local exchange carrier (LEC). Any person engaged in the provision of telephone exchange service or exchange access. Such term does not include a person insofar as such person is engaged in the provision of a commercial mobile service under section 332(c) of TA-96, except to the extent that the Commission finds that such service should be included in the definition of such term.

Opt-in approval. A method for obtaining customer consent to use, disclose, or permit access to the customer's CPNI. This approval method requires that the carrier obtain the customer's affirmative, express consent allowing the requested CPNI usage, disclosure, or access after the customer is provided appropriate notification of the carrier's request.

Opt-out approval. A method for obtaining customer consent to use, disclose, or permit access to the customer's CPNI. Under this approval method, a customer is deemed to have consented to the use, disclosure, or access to the customer's CPNI if the customer has failed to object thereto within the prescribed waiting period, after the customer is provided appropriate notification of the carrier's request for opt-out consent.

Password. A secret word or sequence of alpha and numeric characters which is used to limit access to a customer's account to authorized individuals.

Pretexting. The practice of pretending to be a particular customer or other authorized person in order to obtain access to that customer's call detail or other private communications records.

Readily available biographical information. Information drawn from the customer's life history and includes such things as the customer's social security number, or the last four digits of that number; mother's maiden name; home address; or date of birth.

Subscriber list information (SLI). Any information –

(A) identifying the listed names of subscribers of a carrier's subscribers and such subscribers' telephone numbers, addresses, or primary advertising classifications (as

such classifications are assigned at the time of the establishment of such service), or any combination of such listed names, numbers, addresses, or classifications; and

(B) that the carrier or an affiliate has published, caused to be published, or accepted for publication in any directory format.

Telecommunications Carrier. Any provider of telecommunications services, except that such terms does not include aggregators of telecommunications services (as defined in 47 USC 226).

Telecommunications service. The offering of telecommunications for a fee directly to the public, or to such classes of users as to be effectively available directly to the public, regardless of the facilities used.

Telephone number of record. The telephone number associated with the underlying service, not the telephone number supplied as a customer's "contact information."

Valid photo identification. A government-issued personal identification with a photograph such as a driver's license, passport, or comparable ID that is not expired.

Company Policy Regarding CPNI

The policy of Triangle Telephone Cooperative/Central Montana Communications/Triangle Communication System ("Company") is to comply with the letter and spirit of all laws of the United States, including those pertaining to CPNI contained in §222 of the Telecommunications Act of 1996, as amended, 47 USC 222, and the FCC's regulations, 47 CFR subpart U. The Company's policy is to protect the confidentiality of CPNI and to rely on the involvement of high-level management to ensure that no use of CPNI is made until a full review of applicable law has occurred.

The FCC's regulations, 47 CFR 64.2009, require the Company to implement a system to clearly establish the status of a customer's CPNI approval prior to the use of CPNI; to train its personnel as to when they are, and are not, authorized to use CPNI; and to have an express disciplinary process in place. This Manual constitutes the Company's policies and procedures related to CPNI.

All employees are required to follow the policies and procedures specified in this Manual.

Any questions regarding compliance with applicable law and this Manual should be referred to the Assistant General Manager who has been designated as the CPNI Compliance Officer.

Any violation of, or departure from, the policies and procedures in this Manual shall be reported immediately to the Assistant General Manager or Customer Service Manager.

CPNI in General

What is CPNI?

Customer Proprietary Network Information (CPNI) is information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier, and that is made available to the carrier solely by virtue of the carrier-customer relationship; and information contained in the bills pertaining to telephone exchange service or telephone toll service received by a customer of a carrier. Examples of CPNI include:

- Information regarding to whom, where, and when a customer places a call;
- Frequency, timing, and duration of calls;
- The types of service offerings to which the customer subscribes;
- The extent to which a customer uses a service;
- Call detail information on inbound and outbound calls.
- Total bill due.

CPNI does not include:

- Subscriber list information;
- Customer name, address and phone number;
- Aggregate customer information where individual customer identities and characteristics have been removed.

Use of CPNI in General

The Company has a duty to protect the confidentiality of its customers' CPNI. However, the Company must disclose CPNI upon affirmative written request by the customer, to any person designated by the customer (Form 7).

Except as otherwise permitted as described in this Manual, when the Company receives or obtains CPNI by virtue of a telecommunications service, it can only use, disclose, or permit access to individually identifiable CPNI in its provision of:

1. The telecommunications service from which the information is derived; or
2. Services necessary to, or used in, the provision of the telecommunications service, including the publishing of directories.

When the Company receives or obtains CPNI from another carrier for purposes of providing any telecommunications service, it shall use such CPNI only for such purpose, and not for its own marketing efforts.

Use of CPNI: Customer Approval not Required

The Company may use, disclose, or permit access to CPNI without customer approval:

1. To provide inside wiring installation, maintenance, and repair services.

2. For the provision of customer premises equipment and call answering, voice mail or messaging, voice storage and retrieval services, and protocol conversion.

3. To protect the rights of property of the Company, or to protect users of those services and other carriers from fraudulent, abusive, or unlawful use of, or subscription to, such services;

4. To initiate, render, bill and collect for telecommunications services;

5. To provide or market service offerings among the categories of service (i.e., local, long distance, and CMRS (wireless) to which the customer already subscribes from the company. For example, if a customer subscribes to local exchange service of Triangle Telephone Cooperative, Triangle Telephone Cooperative may use CPNI to market local exchange service calling plans to the customer;

6. If a company provides different categories of service, and a customer subscribes to more than one category of service offered by that company, the company may share CPNI among its affiliated entities that provide a service offering to the customer;

7. To market services formerly known as adjunct-to basic services such as, but not limited to, speed dialing, call acceptance, call rejection, priority calling, teen ring, speed calling, voice mail, call waiting, caller ID, and call forwarding.

Use of CPNI: Customer Approval Required

The Company may not use, disclose, or permit access to CPNI to market service offerings to a customer that are within a category of service to which the customer does not already subscribe from the Company unless customer approval is not necessary (as described above) or the Company has customer approval to do so.

If one of the Companies provides different categories of service, but a customer does not subscribe to more than one offering by that Company, the Company is not permitted to share CPNI with its affiliates, except with the customer's approval (see item 6 above).

Obtaining Customer Approval for Use of CPNI

The Company may obtain customer approval through written or oral methods. The Company has determined that it will not use electronic methods as a means of providing notification to customers relative to CPNI. If the Company relies on oral approval, it bears the burden of demonstrating that such approval has been given in compliance with the FCC's regulations.

A customer's approval or disapproval to use, disclose, or permit access to CPNI will remain in effect until the customer revokes or limits such approval or disapproval. The Company will maintain records of approval, whether oral, written or electronic, for at least one year.

The Company will utilize the opt-out method to obtain approval to use its customer's individually identifiable CPNI for marketing communications-related services to that customer. The Company will not share individually identifiable CPNI with third parties, joint venture partners or independent contractors other than for the billing and provisioning of telecommunications services. The Company will not use the opt-out method to obtain approval to market non-communications related services to a customer.

Notice Requirements

Prior to requesting customer approval to use, disclose, or permit access to customer's CPNI, the Company must notify the customer of the customer's right to restrict use of, disclosure of, and access to, the customer's CPNI. This notification must provide sufficient information to enable the customer to make an informed decision whether to permit a carrier to use, disclose, or permit access to the customer's CPNI. In addition, the Company's solicitation for approval must be proximate to the notification of a customer's CPNI rights (Form 3). Specifically, the notification must:

a. State that the customer has the right, and the Company has a duty, under federal law, to protect the confidentiality of CPNI.

b. Specify the types of information that constitute CPNI and the specific entities that will receive the CPNI, describe the purposes for which CPNI will be used, and inform the customer of the right to disapprove those uses, and deny or withdraw access to CPNI at any time.

c. Advise the customer of the precise steps the customer must take in order to grant or deny access to CPNI, and must clearly state that a denial of approval will not affect the provision of any services to which the customer subscribes. However, the Company may provide a brief statement, in clear and neutral language, describing consequences directly resulting from the lack of access to CPNI. This may include a statement that the customer's approval to use CPNI may enhance its ability to offer products and services tailored to the customer's needs.

d. Be comprehensible and not misleading. If written notification is provided, the notice must be clearly legible, use sufficiently large type, and be placed in an area so as to be readily apparent to a customer.

e. State that any approval or denial for the use of CPNI outside of the service to which the customer already subscribes from the Company is valid until the customer affirmatively revokes or limits such approval or denial.

f. May state that the company may be compelled to disclose CPNI to any person upon affirmative written request by the customer.

g. May not include any statement attempting to encourage a customer to freeze third-party access to CPNI.

Opt-out Notice Requirements

The Company will provide notification to obtain Opt-out approval through written methods only.

In addition to the notification requirements outlined above, the Company must wait a 30-day minimum period of time after giving customers notice and an opportunity to opt-out before assuming customer approval to use, disclose, or permit access to CPNI. The Company must notify customers as to the applicable waiting period for a response before approval is assumed. When the notification is sent by mail, the waiting period begins to run on the third day following the date that the notification was mailed.

If the Company uses the opt-out mechanism it must provide notices to its customers every two years (Form 3).

One-time Use of CPNI Notice Requirements

The Company may use oral notice to obtain limited, one-time use of CPNI for inbound and outbound customer telephone contacts for the duration of the call. The contents of any such notification must comply with the requirements of items a.-g. above, except that the Company may omit any of the following if not relevant to the limited use for which the carrier seeks CPNI:

a. The Company need not advise customers that if they have opted-out previously, no action is needed to maintain the opt-out election.

b. The Company need not advise customers that it may share CPNI with its affiliate(s) or third parties and need not name those entities, if the limited CPNI usage will not result in use by, or disclosure to, an affiliate or third party.

c. The Company need not disclose the means by which a customer can deny or withdraw future access to CPNI, so long as the Company explains to customers that the scope of the approval the Company seeks is limited to one-time use.

d. The Company may omit disclosure of the precise steps a customer must take in order to grant or deny access to CPNI, as long as the Company clearly communicates that the customer can deny access to his CPNI for the call.

Company Safeguards

The CPNI Compliance Officer will oversee the use of approval methods and notice requirements for compliance with all legal requirements.

All marketing and sales campaigns must first be reviewed and approved (Form 2) by the CPNI Compliance Officer, who will also store copies of all marketing and sales materials in the CPNI files. In deciding whether the contemplated use of the CPNI is proper, the CPNI Compliance Officer will consult applicable FCC regulations and, if necessary, legal counsel.

The Company will review this CPNI Manual and Procedures on a continuing basis (at least annually) to ensure compliance with all FCC regulations, and will revise these procedures as needed to reflect any subsequent revisions to the applicable rules and regulations addressing CPNI. The review may include a review of this Manual and related procedures with the Board of Directors.

Employee Training

Training of all Company personnel will include review of this Manual by all new employees and all existing employees who have not previously done so. The Company will provide additional training on an as-needed basis on the proper use and disclosure of CPNI. The Company also provides a copy of this Manual on the company's internal website for employee reference. Documentation of training (Form 1) will be kept on file for a period of at least five years.

Any improper use of CPNI will be reported to the General Manager and a record will be made of the infraction(s) and the disciplinary steps taken in accordance with established Company disciplinary procedures. Depending on the circumstances of the violation (including the severity of the violation, whether the violation was a first time or repeat violation, and the extent to which the violation was or was not deliberate or malicious), the disciplinary action may include additional training to ensure future compliance, reprimand, and/or termination as well as other actions.

Access to CPNI

Access to Customer Proprietary Network Information (CPNI) data is limited to employees with the requisite proper authorization as allowed by FCC rules. Any employee with CPNI access must operate under the policies outlined in this Manual that require protection of confidential information. Improper use or disclosure of CPNI by employees is subject to disciplinary action up to and including termination.

FCC Notification of Opt-out Failure

The Company will provide written notice to the FCC within five business days of any instance where the opt-out mechanisms did not work properly to such a degree that the customer's inability to opt-out is more than an anomaly. The notice will be in the form of a letter (Form 4), and will include the Company's name, a description of the opt-out mechanism(s) used, the problem(s) experienced, the remedy proposed and when it will be/was implemented, whether the state commission has been notified and whether it has taken any action, a copy of the notice provided to customers (Form 5), and contact information.

The notice will be sent to the FCC even if the Company offers other methods by which consumers may opt-out.

Annual Filing of Certificate of Compliance

On an annual basis, a corporate officer of the Company will sign and file with the FCC a Compliance Certificate (Form 9) stating to his or her personal knowledge that the Company has established operating procedures that are adequate to ensure comply with the FCC's CPNI rules. This certification will be made publicly available by request.

In addition to the annual certification, the Company will provide an accompanying statement explaining how the Company's operating procedures ensure that it is or is not in compliance with the FCC's CPNI rules as well as an explanation of any actions taken against data brokers and a summary of all Customer complaints received in the past year concerning the unauthorized release of CPNI. Additionally, the Company must report on any information it has with respect to the processes pretexters are using to attempt to access CPNI and what steps it is taking to protect CPNI.

The "actions against data brokers" discussed above refers to proceedings instituted or petitions filed by the Company at either a state or federal commission or the court system.

The "summary of all customer complaints received" refers to the number of customer complaints the Company has received related to unauthorized access to CPNI, or unauthorized disclosure of CPNI, broken down by category of complaint, e.g., instances of improper access by employees, instances of improper disclosure to individual not authorized to receive the information, or instances of improper access to online information by individuals not authorized to view the information.

This annual filing will be made with the FCC's Enforcement bureau on or before March 1 in EB Docket No. 06-36, for data pertaining to the previous calendar year.

Interface with Contractors

The Company has occasion to utilize contractors for specific projects/services needed to conduct its business. The Company requires all its contractors who may have access to CPNI to include language similar to the following in all agreements:

"Whereas Triangle Telephone Cooperative is required by law and its company policies to protect the privacy and security of the information regarding its customers, to the extent that Contractor, in rendering services for Triangle Telephone Cooperative receives customer proprietary network information, as that term is defined under 47 U.S.C. Section 222 and interpreted by the FCC ("CPNI"), Contractor shall maintain the confidentiality of such CPNI according to the policies and procedures implemented by Triangle Telephone Cooperative. Contractor shall promptly delete from its records any CPNI that is received by Contractor in its engagement with Triangle Telephone Cooperative when it is no longer needed in the performance of this agreement."

Recordkeeping Requirements

The Company will maintain records (Form 2) of its own sales and marketing campaigns and of its affiliates' sales and marketing campaigns that use CPNI in files clearly identified as such. These records include a description of each campaign, the specific CPNI that was used in the campaign, and the products and services that were offered as a part of the campaign. The Company will maintain these records in its offices for a minimum of one year.

The Company maintains records which clearly establish customer approval for use of CPNI, as well as notices required by the FCC's regulations for a minimum of one year. The Company maintains records of customer approval and disapproval for use of CPNI in a readily-available location that is consulted on an as-needed basis.

All customer complaints concerning the unauthorized release of CPNI will be logged (Form 6) and retained for a period of five years. This information is summarized and included with the Company's annual certification to the FCC.

The Company will maintain separate files in which it will retain court orders requiring disclosure of CPNI.

Authentication and Procedural Safeguards

The Company will take reasonable measures to discover and protect against attempts to gain unauthorized access to CPNI including pretexting. These measures include properly authenticating a customer prior to disclosing CPNI and vary depending on whether the disclosure is via customer initiated telephone contact, online account access, or an in-store visit. In all cases, the requesting party must be on the account as a member/responsible party or an Authorized Account Representative (AAR) to access any customer account information (Form 7).

Establishment of a Password

The Company authenticates the customer without the use of readily available biographical or account information. The Company established passwords upon implementation of these procedures by supplying the customer with a randomly-generated personal identification number (PIN), not based on readily available biographical information or account information, which the customer then provides to the Company prior to establishing a password. The Company initially supplied the PIN to the customer by mailing it to the address of record and subsequently may provide it by voice to the telephone number of record or by mailing it to the address of record.

New customers will be required to establish their password at the time of service initiation.

Establishment of a Back-up Authentication Method

The Company may create a back-up customer authentication method in the event of a lost or forgotten password. The back-up customer authentication method may not prompt the customer for readily available biographical information or account information.

The use of security questions is the preferred back-up authentication method (Form 7). If the customer cannot provide the correct password, the customer must answer at least two of the security questions correctly prior to disclosing any CPNI information.

If a customer cannot provide the correct password or the correct responses for the back-up customer authentication method, the customer must establish a new password (Form 9).

Customer Initiated Telephone Access to CPNI

Release of any CPNI information requested by the customer via a telephone call is allowed when:

- The requesting individual provides the password of record; or
- The information will be sent via United States Postal Service to the customer's address of record; or
- The Company representative calls the telephone number of record and discloses the requested information to the customer or authorized representative.

If the customer has forgotten their password but can provide the call detail information in question, the Company can proceed with routine customer care procedures regarding that

specific call detail information only. The Company will not disclose any call detail other than the information the customer disclosed during that particular contact.

Retail Location Account Access

Customers or their authorized account representative must present a valid, government issued photo identification, such as a driver's license, passport, or comparable ID or provide the CPNI password of record to obtain CPNI information at a retail location.

On-line Account Access

The Company requires an on-line password to protect on-line access to all CPNI, not just call detail records. Customers seeking on-line access to their CPNI will be authenticated prior to establishment of the on-line password. The authentication process consists of the customer entering their CPNI password, account number and number of record to establish an on-line account.

On-line passwords are designed by the customer and consist of alpha and/or numeric characters with a maximum length of 13 characters. The Company can reinitialize existing passwords for on-line access but will not base on-line passwords on readily available biographical or account information.

On-line access to CPNI will be blocked after five (5) unsuccessful attempts to log on. The customer will be required to contact the Company to be reauthenticated prior to reactivating the on-line access.

Notification of Account Changes

After an account is established, the Company will notify (Form 8) a customer immediately of any account changes including password, customer response to Company designed back-up means of authentication, on-line account, or address of record is created or changed. This notification may be through a voice message to the telephone number of record or by United States Postal Service to the address of record as it was prior to the change. The notification will not reveal the changed information.

Notification of CPNI Security Breaches

The Company will take reasonable steps to protect CPNI databases from hackers and other unauthorized attempts by third parties to access CPNI.

The Company shall not notify its customers or disclose the breach publicly, whether voluntarily or under state or local law or these rules, until it has completed the process of notifying law enforcement.

As soon as practicable, and in no event later than seven (7) business days after a reasonable determination that a breach has occurred, the Company will notify law enforcement of any CPNI breaches. The Company will send an electronic notification through the central reporting facility to the United States Secret Service (USSS) and the Federal Bureau of Investigation (FBI). This will be done through the FCC's link to the reporting facility at http://www.fcc.gov/eb/cpni. The Company will request authorization via the central reporting facility to notify its customer(s) immediately if desired. Responsibility to notify USSS and FBI has been assigned to the General Manager or CPNI Compliance Officer.

After the Company has completed the process of notifying law enforcement as listed above, it shall notify its customers of a breach of those customers' CPNI. Notwithstanding any state law to the contrary, the Company shall not notify customers or disclose the breach to the public until seven (7) full business days have passed after notification to the USSS and the FBI except as in the following two situations.

a) If the Company believes that there is an extraordinarily urgent need to notify any class of affected customers sooner than otherwise allowed under the above paragraph of this section, in order to avoid immediate and irreparable harm, it shall so indicate in its notification and may proceed to immediately notify its affected customers only after consultation with the relevant investigating agency. The Company shall cooperate with the relevant investigating agency's request to minimize any adverse effects of such customer notification.
b) If the relevant investigating agency determines that public disclosure or notice to customers would impede or compromise an ongoing or potential criminal investigation or national security, such agency may direct the Company not to disclose or notify for an initial period of up to 30 days. Such period may be extended by the agency as reasonably necessary in the judgment of the agency. If such direction is given, the agency shall notify the Company when it appears the public disclosure or notice to affected customers will no longer impede or compromise a criminal investigation or national security. The agency shall provide in writing its initial direction to the Company, any subsequent extension, and any notification that notice will no longer impede or compromise a criminal investigation or national security and such writing shall be contemporaneously logged on the same reporting facility that contains records of notifications filed by carriers.

The Company will maintain a record, electronically or in some other manner, of any breaches discovered, notifications made to the USSS and the FBI as defined in the above section (Form 10), and all notifications made to customers (Form 11). This record must include, if available, the dates of discovery and notification, a detailed description of the CPNI that was the subject of the breach, and the circumstances of the breach. The Company will retain the record for a minimum of 2 years.

This section does not supersede any statute, regulation, order, or interpretation in any State, except to the extent that such statute, regulation, order, or interpretation is inconsistent with the provisions of this section, and then only to the extent of the inconsistency.